Integrated Public Alert and Warning System's

(IPAWS)

Geo-Targeted Alerting System

(GTAS)

Pilot Project Risk Mitigation Plan

February 19, 2010

Version 1.1

NOAA/OAR/ESRL
Global Systems Division
Information Systems Branch

Boulder, CO

Contents

Purpose

This document is written to identify, categorize, prioritize, and develop risk mitigation strategies associated with the development and operations of the Integrated Public Alert and Warning System's (IPAWS) Geo-Targeted Alerting System (GTAS) pilot project. This is a living document that will evolve as risks are identified and mitigated.

Introduction

GTAS is sponsored by the Department of Homeland Security (DHS) and is a joint development effort between the National Oceanic and Atmospheric Administration's (NOAA) Earth System Research Laboratory (ESRL) Global Systems Division (GSD), NOAA's Air Resource Laboratory (ARL), and the National Ocean Service's (NOS) Office of Response and Restoration (ORR). GTAS is a rapid development and deployment effort that integrates the latest research efforts in dispersion and high resolution weather models into a network enabled shared situational awareness display system. GTAS will improve communication and coordination between local Emergency Operations Centers (EOC) emergency managers and National Oceanic and Atmospheric Administration's (NOAA) National Weather Service (NWS) Weather Forecast Office (WFO) meteorologists during severe weather, natural disasters, toxic spills, and terrorist attacks to help reduce loss of life and property. GTAS will do this by providing all users the ability to:

- Run and view dispersion of toxic plumes.
- View hazardous weather information.
- Coordinate and collaborate between agencies.
- Assess societal impacts due to toxic chemical releases and severe weather conditions.
- Disseminate societal impact information.

GSD and DHS have identified 5 potential pilot sites for demonstrating GTAS capabilities.

- Dallas/Fort Worth
- Seattle
- Kansas City
- New York City
- Washington D.C.

The sites were chosen based partly on the potential risk of severe weather, or terrorist attack. GTAS will be comprised of many client systems communicating through the internet to a server (see figure 1). The GTAS server is responsible for providing access to:

- Real-time weather observations and forecasts.
- Dispersion model activation.
- Dispersion model output.
- Collaboration for shared situational awareness.

GTAS will leverage the existing NWS network infrastructure and weather display systems to provide the GTAS server with the real-time weather display capabilities. The NWS infrastructure provides a pathway

to national deployment if the GTAS pilot project is a success. GTAS will also leverage existing hardware and communications capabilities at each of the client sites to host the GTAS client application.

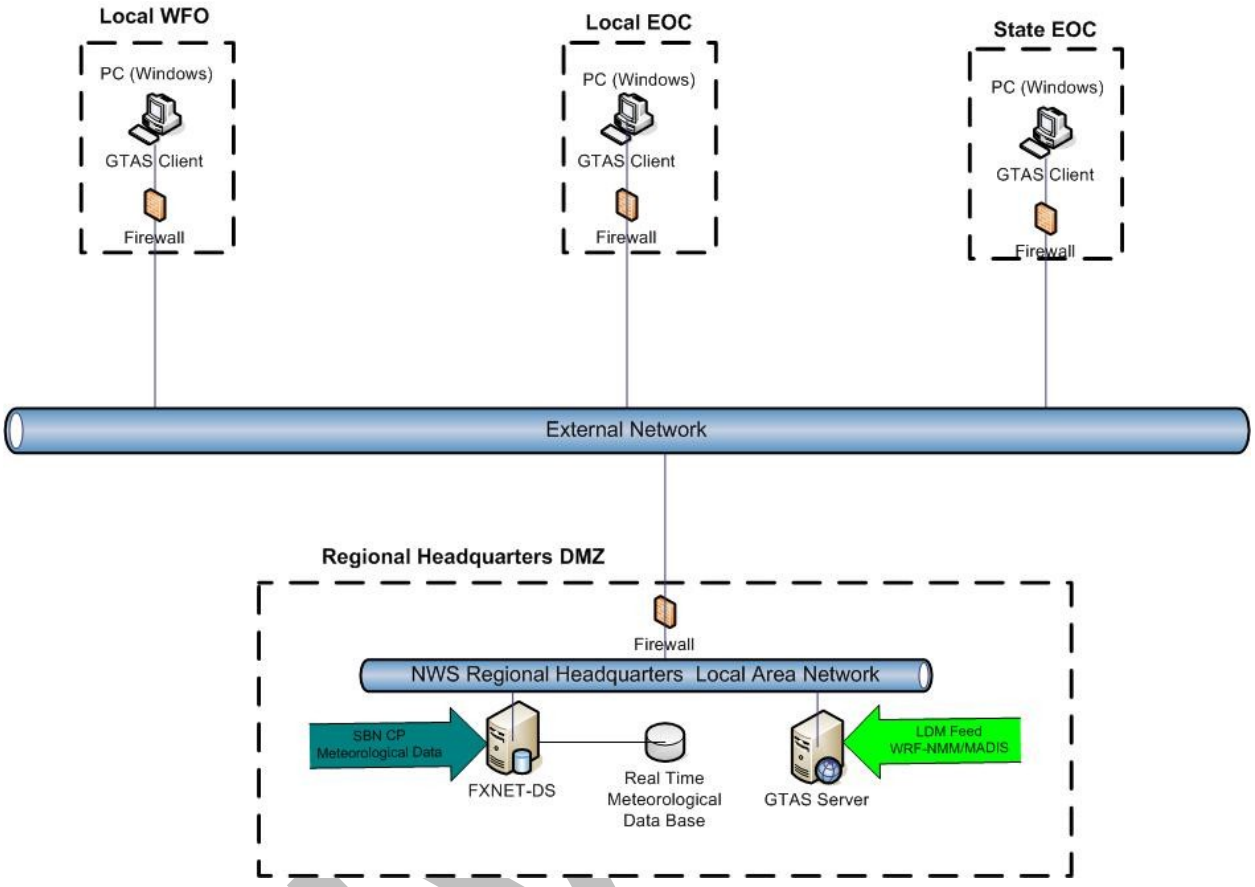

Figure 1

Basic System Architecture

Project Objectives

The GTAS pilot project objectives are to:

- Improve how state and local governments use high resolution weather and toxic plume model information for emergency preparedness to help reduce loss of life and property.
- Develop requirements for the NWS Operational Systems Improvement Process (OSIP) to meet GTAS needs.

Identified Risks

The risks identified below are based on knowledge gained in developing and deploying similar systems to operational sites and risks identified with the objectives of the GTAS project.

1. Five pilot sites may not be enough sites to establish requirements for all State and Local governments.
2. Staff changes could realign focus at a state or local EOC.
3. Failure of the GTAS server during an emergency.
4. Participants unable to participate during an actual or staged emergency.
5. GTAS participant is unavailable during information gathering for evaluations.
6. Site doesn't want to participate or have the time to participate.
7. GTAS interface not easy to use during emergency operations.
8. Developers do not fully understand a user requirement.
9. High Performance Computing system goes down or unavailable to make WRF-NMM model runs.
10. High Performance Computing resources insufficient to make all forecast runs for all sites.
11. Bandwidth at NWS regional headquarters not large enough to accept all WRF-NMM model data.
12. Communications fail during send of WRF-NMM model data to the GTAS servers.
13. GTAS server is over utilized to run the dispersion model.
14. WRF-NMM data not available on the GTAS server when dispersion model is run.
15. Internet communications goes down or is over utilized during the request to run and display the dispersion model data.
16. Too many applications running on GTAS client to handle display of dispersion model data during an event.
17. User unable to create CAP messages from warning boxes on GTAS client interface.
18. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.
19. Client sites may not have the internet bandwidth to support GTAS client communications.
20. Sites may not allow internet communications for security reasons.
21. NWS infrastructure at regional headquarters may not be able to support access to meteorological data sets by the GTAS server.
22. NWS regional headquarters may have limited bandwidth for the support of GTAS communications.
23. GTAS server deliveries delayed to regional headquarters.
24. Regional headquarters slow to install GTAS server.
25. Sites slow in getting security approvals for GTAS.

Categorized Risks

All GTAS risks fall into one or more of the following five categories:

- Human Resources
- Objective
- Budget
- Schedule
- Technical

Human Resource Risks

The GTAS pilot project will be implemented at four NWS regional headquarters, four NWS WFOs, NOAA headquarters, five local EOCs, and 4 state EOCs. These facilities are not being provided extra funding, staffing, or equipment to help with this effort. Human resource risks for the GTAS project are:

1. Staff changes could realign focus at a state or local EOC.
2. Participants unable to participate during an actual or staged emergency.
3. GTAS participant is unavailable during information gathering for evaluations.
4. Staff changes could realign focus at a state or local EOC.

Objective Risks

Objective risks for GTAS are those risks associated with improving how state and local governments use high resolution weather and toxic plume model information for emergency preparedness and developing GTAS requirements for NWS OSIP.

1. Five pilot sites may not be enough sites to establish requirements for all State and Local governments.
2. Developers do not fully understand a user requirement.
3. GTAS participant is unavailable during information gathering for evaluations.
4. Site may not want to participate or not have the time to participate.
5. Staff changes could realign focus at a state or local EOC.
6. Participants unable to participate during an actual or staged emergency.
7. Failure of the GTAS server during an emergency.
8. GTAS interface not easy to use during emergency operations.
9. High Performance Computing system goes down or unavailable to make WRF-NMM model runs.
10. GTAS server is over utilized to run the dispersion model.
11. Internet communications goes down or is over utilized during the request to run and display the dispersion model data.
12. Too many applications running on GTAS client to handle display of dispersion model data during an event.
13. User unable to create CAP messages from warning boxes on GTAS client interface.

Budget Risks

Budget risks are risks that could cause an increase in the cost of the GTAS pilot project.

1. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.
2. Client sites may not have the internet bandwidth to support GTAS client communications.
3. GTAS participant is unavailable during information gathering for evaluations.
4. Site may not want to participate or not have the time to participate.
5. Staff changes could realign focus at a state or local EOC.
6. NWS infrastructure at regional headquarters may not be able to support access to meteorological data sets by the GTAS server.
7. GTAS server is over utilized to run the dispersion model.
8. Sites may not allow internet communications for security reasons.

9. NWS regional headquarters may have limited bandwidth for the support of GTAS communications.

Schedule Risks

Schedule risks are risks that would cause the project tasking timelines to be extended.

1. GTAS server deliveries delayed to regional headquarters.
2. Regional headquarters slow to install GTAS server.
3. Sites slow getting security approvals for GTAS.
4. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.
5. Client sites may not have the internet bandwidth to support GTAS client communications.
6. Sites may not allow internet communications for security reasons.
7. NWS infrastructure at regional headquarters may not be able to support access to meteorological data sets by the GTAS server.
8. GTAS participant is unavailable during information gathering for evaluations.
9. Site may not want to participate or not have the time to participate.
10. Staff changes could realign focus at a state or local EOC.
11. GTAS server is over utilized to run the dispersion model.
12. NWS regional headquarters may have limited bandwidth for the support of GTAS communications.

Technical Risks

Technical risks are risks that are associated with the operational use of the GTAS server and client systems during real or simulated events.

1. Failure of the GTAS server during an emergency.
2. GTAS interface not easy to use during emergency operations.
3. High Performance Computing system goes down or unavailable to make WRF-NMM model runs.
4. High Performance Computing resources insufficient to make all forecast runs for all sites.
5. Bandwidth at NWS regional headquarters not large enough to accept all WRF-NMM model data.
6. Communications fail during send of WRF-NMM model data to the GTAS servers.
7. GTAS server is over utilized to run the dispersion model.
8. WRF-NMM data not available on the GTAS server when dispersion model is run.
9. Internet communications goes down or is over utilized during the request to run and display the dispersion model data.
10. Too many applications running on GTAS client to handle display of dispersion model data.
11. User unable to create CAP messages from warning boxes on GTAS client interface.
12. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.
13. Client sites may not have the internet bandwidth to support GTAS client communications.
14. Sites may not allow internet communications for security reasons.

Prioritized Risks

Priority for mitigation was determined by assigning each risk two values:

1. Probability of occurrence was determined by GSD's past experience at installing prototype systems at operational facilities in support of operations and the number of times a risk appeared in the category lists above.
2. Project impact risk values were assigned based on the ability for GSD to meet project goals if the risk became a reality.

The probabilities of occurrence values have the following meanings:

Probability Values

Score	Meaning
1	Not likely to occur
2	Might occur
3	Most likely will occur
4	Definitely will occur

Table 1

The impact values have the following meanings:

Impact Values

Score	Meaning
1	User trust and is willing to continue using the system. Adjustments to documentation or user processes may be required.
2	User trust and is willing to use the system. Minor adjustments to the GTAS system are required
3	User believes in system but is not willing to use the system unless major code and documentation changes are made.
4	User is not sure if this is the correct approach for their emergency decision support needs. Major architectural changes are required for user support.
5	User believes that GTAS impedes the emergency decision support process and is unwilling to continue with the pilot project.

Table 2

Total Risk or Assessed Risk

Score	Meaning	GTAS

		Priority
1-2	Risk will not impact project goals and requirements.	NCD
3-4	Risks if not addressed with a mitigation strategy may cause delays in meeting project goals.	3
5-6	Risks if not addressed with a mitigation strategy will cause delays in meeting project goals.	2
7 or Greater	Risks if not addressed with a mitigation strategy will cause the GTAS project to fail.	1

Table 3

Risk Assessment

Risk	Probability Value	Impact Value	Total Risk
1. Five pilot sites may not be enough sites to establish requirements for all State and Local governments.	4	1	5
2. Staff changes could realign focus at a state or local EOC.	2	1	3
3. Failure of the GTAS server during an emergency.	2	5	7
4. Participants unable to participate during an actual or staged emergency.	2	4	6
5. GTAS participant is unavailable during information gathering for evaluations.	2	4	6
6. Site doesn't want to participate or have the time to participate.	1	4	5
7. GTAS interface not easy to use during emergency operations.	2	3	5
8. Developers do not fully understand a user requirement.	1	3	4
9. High Performance Computing system goes down or unavailable to make WRF-NMM model runs.	1	1	2
10. High Performance Computing resources insufficient to make all forecast runs for all sites.	1	2	3
11. Bandwidth at NWS regional headquarters not large enough to accept all WRF-NMM model	2	2	4

data.			
12. Communications fail during send of WRF-NMM model data to the GTAS servers.	1	1	2
13. GTAS server is over utilized to run the dispersion model.	1	4	5
14. WRF-NMM data not available on the GTAS server when dispersion model is run.	1	1	2
15. Internet communications goes down or is over utilized during the request to run and display the dispersion model data.	2	3	5
16. Too many applications running on GTAS client to handle display of dispersion model data during an event.	2	2	4
17. User unable to create CAP messages from warning boxes on GTAS client interface.	1	5	6
18. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.	2	3	5
19. Client sites may not have the internet bandwidth to support GTAS client communications.	2	3	5
20. Sites may not allow internet communications for security reasons.	2	3	5
21. NWS infrastructure at regional headquarters may not be able to support access to meteorological data sets by the GTAS server.	1	4	5
22. NWS regional headquarters may have limited bandwidth for the support of GTAS communications.	1	4	5
23. GTAS server deliveries delayed to regional headquarters.	1	1	2
24. Regional headquarters slow to install GTAS server.	2	3	5
25. Sites slow in getting security approvals for GTAS.	2	3	5
Average Scores:	1.64	2.8	4.44

Table 4

Risk Mitigation Strategies

Risk mitigation approaches will be described for any risks that are at a total risk level of 3 or higher. Lower level risks are Not Considered Detrimental (NCD) to the GTAS pilot project.

Priority 1 Risks – Total Risk Factor 7 or Greater

1. Failure of the GTAS server during an emergency.

Mitigation Strategy

1) Add GTAS backup servers that are located at different physical locations then the primary GTAS servers. GSD will provide limited backup support for fielded systems in 2009. This will start to be addressed in out years if funding permits.
2) Exercise the primary and backup servers on a daily basis to verify:
    a. Network connectivity.
    b. Firewall access to GTAS services and clients.
    c. Meteorological and dispersion data availability.
3) The Seattle EOC is holding an infrastructure attack scenario in May of 2010. GTAS and GSD should be a part of this to help identify and mitigate infrastructure attack risks. (10/27/09).
4) The Seattle WFO wants to host the backup server for Western Region. Since Western Region Headquarters is supplying their own GTAS server the server we purchased will be configured to run at the Seattle WFO.

Priority 2 Risks – Total Risk Factor 5 or 6

2. Participants unable to participate during an actual or staged emergency.

Mitigation Strategy

1) Train as many personnel as possible at all client site locations.
2) Hold simulation and practice exercises to help gather feedback and promote the use of GTAS for operations.
3) Determine why participants weren't able to participate and work with site to fix problem.

3. GTAS participant is unavailable during information gathering for evaluations.

Mitigation Strategy

1) Try and gather feedback following every exercise.
2) Allow users to give feedback online when they have the time.
3) Perform phone interviews if the clients are willing.

~~4. User unable to create CAP messages from warning boxes on GTAS client interface.~~ GTAS has been tested and is CAP version 1.1 compliant. Will retest for version 1.2 once CAP version 1.2 is available.

Mitigation Strategy

1) Document the process for creating a CAP message.
2) Train users on the CAP message creation process.
3) Make documentation for the CAP message creation process available for users.
4) Have users create CAP messages as part of their recurring training exercises.
5) Test CAP message creation process and verify CAP message version 1.1 compliance.

5. Five pilot sites may not be enough sites to establish requirements for all State and Local governments.

Mitigation Strategy

1) We will push the requirements we do gather into the OSIP process this will at least help how WFO forecasters communicate with local and state EOCs.
2) In follow on years we will continue to add pilot sites.
3) As we find more advanced pilot sites i.e.
   a. Proactive communications between WFO and EOCs not reactive.
   b. Well documented processes in the event of an emergency response.

   this will help us build a template for other states that are still developing an approach or do not have well defined processes.

~~6. Site doesn't want to participate or have the time to participate.~~ All GTAS selected sites have agreed to participate.

Mitigation Strategy

1) We will start with NWS southern region headquarters where we already have good support.
2) Regional headquarters will identify the best WFO in their region to work with.
3) The WFO will then identify the best local EOC.
4) The above template will be used to push GTAS to other regions.
5) Leverage the fact that all participants have the ability to add their requirements into OSIP.
   a. Thin client of the future.
   b. Collaboration of the future.
   c. Decision support tools for the future.
   d. NWS infrastructure of the future.
6) Help sites develop process and graphics that cut time required to brief on event.

7. GTAS interface not easy to use during emergency operations.

Mitigation Strategy

1) GSD will use a circular requirements refining process where requirements are gathered, implemented, fielded, and reevaluated by participants. This will happen with each site installation.
2) Work with sites to determine problem areas with interface and add changes to GTAS for next release of software.
3) Have new releases with each new regional installation with upgrades based on feedback from sites already participating.

8. GTAS server is over utilized to run the dispersion model.

Mitigation Strategy

1) Test system under load.
2) Create process for going from development to operations that tests system loading.
3) Update infrastructure as required to alleviate system loading. This may require out year funding expenditures.
4) Prioritize processes on the system so that the dispersion model has the required resources when run.

9. Internet communications goes down or is over utilized during the request to run and display the dispersion model data.

Mitigation Strategy

1) This is part of what we are trying to determine and fits in with requirements gathering.
2) Work with site to isolate and help mitigate problem if possible.
3) Develop internet communications requirements and recommendations.

10. Client sites (local EOC, local WFO, and state EOC) may not have the hardware to support GTAS client application.

Mitigation Strategy

1) This is part of what we are trying to determine and fits in with requirements gathering.
2) During site coordination and preparation the sites ability to participate will be determined based on minimum requirements list. If the site doesn't meet minimum requirements and can't purchase necessary hardware to meet compliance then we will identify this as a problem and also find a new pilot site that does meet the minimum requirements.

11. Client sites may not have the internet bandwidth to support GTAS client communications.

Mitigation Strategy

1) This is part of what we are trying to determine and fits in with requirements gathering.
2) During site coordination and preparatory work, the site's ability to participate will be determined based on minimum requirements list. If the site doesn't meet minimum requirements and can't purchase necessary hardware to meet compliance then we will identify this as a problem and also find a new pilot site that does meet the minimum requirements.

12. Sites may not allow internet communications for security reasons.

Mitigation Strategy

1) This is part of what we are trying to determine and fits in with requirements gathering.
2) We will work with sites based on the template that we create in southern region which locks downs specific ports to specific ip addresses.
3) Develop GTAS communications that is allowed by all sites based on the use of port 80 for HTTP communications.
4) Continue to develop GTAS to fit into evolving security paradigms.

13. NWS infrastructure at regional headquarters may not be able to support access to meteorological data sets by the GTAS server.

Mitigation Strategy

1) Work with headquarters to determine alternate approaches to acquiring access to the meteorological data sets.
2) Host the primary GTAS servers at GSD.
3) In Central region we will need to purchase a data server because they will not allow us to NFS mount the FX-NET fire weather data server.

14. NWS regional headquarters may have limited bandwidth for the operational support of GTAS communications.

Mitigation Strategy

1) Host the primary GTAS server at GSD.
2) Document this deficiency and what the minimum bandwidth requirements are.

15. Regional headquarters slow to install primary GTAS server.

Mitigation Strategy

1) Host the primary GTAS server for the region in question at GSD until the region is ready to proceed.

16. Sites slow in getting security approvals for GTAS.

Mitigation Strategy

1) Host a server at GSD outside NWS NOAANET until approvals are granted.
2) Work on using HTTP protocol so that this isn't an issue in the future.

Priority 3 Risks – Total Risk Factor 3 or 4

17. Developers do not fully understand a user requirement.

Mitigation Strategy

1) GSD will use a circular requirements refining process where requirements are gathered, implemented, fielded, and reevaluated by participants. This will happen with each site installation. As this is a repetitive process developers through this rapid feedback process will continue to refine their understanding of participant needs.
2) Have developers involved in talking with participants if there are misunderstandings in requirements.

18. Bandwidth at regional headquarters not large enough to accept full WRF-NMM model data runs.

Mitigation Strategy

1) We will reduce the number of fields to the minimum number of data fields to support HySPLIT runs.
2) We will reduce the temporal resolution of the WRF-NMM data.
3) We will reduce the spatial domain of the WRF-NMM model in the vertical dimension.
4) HySPLIT will be engineered in the GTAS system to use high-resolution weather models available at regional headquarters as a backup to the WRF-NMM model.

19. Too many applications running on GTAS client to handle display of dispersion model data during an event.

Mitigation Strategy

1) Set priority of GTAS client to the highest allowed run priority level on the client system.
2) Develop strategies with the participants for shutting down unneeded applications on the GTAS client systems during an event.

20. Staff changes could realign focus at a state or local EOC.

Mitigation Strategy

1) Work with new staff at the state or local EOC to develop an understanding of why being a part of the GTAS pilot project is important to the success of their mission.
2) Have the WFO pick a new local EOC to work with.
3) Develop the ability for field sites to come on line and be trained by GTAS pilot participants in the region in question.

~~21. High performance computing resources insufficient to make all WRF-NMM runs for all sites.~~ Model runs for all client sites now running on GSD's high performance computer system.

Mitigation Strategy

1) Part of our tasking is to determine the resources necessary to support this type of dispersion model accuracy; we can do this by supporting just one regional run on the high performance computing system.
2) Have pilot sites run the WRF-NMM model locally.
3) Have the ability to run the HySPLIT dispersion model using other meteorological models.